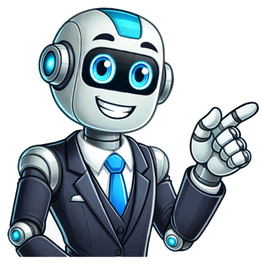
Click to verify



On Wednesday, a jury in New York convicted ex-Central Intelligence Agency engineer Joshua Schulte on all nine charges he faced (as first reported by @InnerCityPress) as a result of the single largest leak in agency history. Dubbed Vault 7, the files and information shared by WikiLeaks in 2017 exposed a trove of tactics and exploits the CIA used to hack its targets computers, iPhones or Android phones, and even Samsung smart TVs.CIA spokesperson Tammy Thorp said in a statement given to The Verge, Todays verdict affirms that maintaining the security of our nations cyber capabilities is of the utmost importance. Its critical to the security of the American people, and its critical to our advantage against adversaries abroad. As set forth in the trial, unauthorized disclosures not only jeopardize US personnel and operations, but also equip our adversaries with tools and information to do us harm.Schulte, the subject of a lengthy profile in the New Yorker that described him as abrasive and then went into far worse details, was arrested in 2018, initially charged with possession of child pornography, and has been in jail ever since.The article details Operations Support Branch (OSB), where Schulte worked and reportedly built hacking tools by quickly turning prototypes into actual exploits that could monitor or steal information from the targeted persons devices. It reports that investigators obtained evidence against Schulte through his own lapses in personal security, like storing passwords on his phone that could be used to access his encrypted storage.It even goes into the trouble investigators had obtaining the Vault 7 documents they remained classified despite being leaked and publicly available on the internet, leading FBI officials to download the cache over Wi-Fi at a Starbucks to a freshly purchased laptop that immediately became officially classified, stored in a supervisors office, and only accessible with Top Secret clearance.Additional charges accusing him directly of stealing classified national defense information and sending it to WikiLeaks were filed later. In 2020, the governments first attempt at prosecuting Schulte ended in a mistrial as a jury convicted him on contempt of court charges as well as lying to FBI investigators but couldnt agree on the rest.That spurred the second trial that just ended, where Schulte opted to represent himself. The charges he was convicted on are all specifically related to gathering, stealing, and transmitting classified information and obstruction of justice for lying to investigators about it. He has not yet been sentenced, pending the resolution of the other charges he still faces for possessing and transporting child pornography.The Associated Press reports prosecutors argued that after feeling ignored and disrespected over his complaints about the work environment, Schulte took revenge on the CIA by stealing and leaking the same exploits hed been a part of creating. In his defense, Schulte argued unsuccessfully that he was being used as a scapegoat for the governments failure to protect dangerous hacking tools. There is some evidence to support that argument, as The Washington Post reported in 2020 that an internal investigation by the CIAs WikiLeaks Task Force found security in the unit was woefully lax, with users sharing admin-level passwords and a lack of controls over access to historical data or the use of removable USB thumb drives, and this was years after the Snowden leaks. Schulte claimed there was no reasonable motive established and that hundreds of people had access to the information who couldve been behind the leaks.In a statement released after the verdict, US Attorney for the Southern District of New York Damian Williams said, When Schulte began to harbor resentment toward the CIA, he covertly collected those tools and provided them to WikiLeaks, making some of our most critical intelligence tools known to the public and therefore, our adversaries. His statement ended by saying, Schulte has been convicted for one of the most brazen and damaging acts of espionage in American history.See More: A man convicted of carrying out one of the most damaging data breaches in the CIA's history the public disclosure of secret hacking tools was sentenced to 40 years in federal prison Thursday, prosecutors said.Former CIA officer Joshua Adam Schulte, 35, was convicted of the so-called Vault 7 leak, and also of possessing child sexual abuse images, in two trials in 2022 and 2023.Damian Williams, U.S. Attorney for the Southern District of New York in Manhattan, said Thursday that Schulte betrayed his country."He caused untold damage to our national security in his quest for revenge against the CIA for its response to Schultes security breaches while employed there," Williams said in a statement after the sentence was imposed.Prosecutors had asked for a life sentence.Schulte, who left the CIA in 2016, stands convicted of some of the most heinous, brazen violations of the Espionage Act in American history, prosecutors said in theirsentencing memoto the judge, adding that he stole an arsenal of extremely sensitive intelligence-gathering cyber-tools from the CIA and handed it to WikiLeaks, which in turn publicized it to Americas adversaries in 2017.The defense asked for nine years,saying that Schulte has been subjected to continuous torture during his six-year confinement since his arrest, and calling him a bright, kind young man whose crimes represent aberrant behavior in an otherwise law-abiding life.Schultes attorney, Csar de Castro, said they hoped for a lighter sentence but were relieved the 40-year sentence was not longer.We are very disappointed that Mr. Schulte received 40 years imprisonment, however, relieved that he did not receive life imprisonment as strongly urged by the government, he said. Joshua Adam Schultevia LinkedInIn aletterto the court, Deputy CIA Director David Cohen called the leak one of the largest unauthorized disclosures of classified information in the history of the United States and said it caused exceptionally grave harm to U.S. national security.He said the leak placed directly at risk CIA personnel, programs, and assets.Evidence at the trial showed Schulte worked for an elite CIA hacking unit, became disgruntled at work and may have leaked the material in a spiteful attempt to lash back at his colleagues.After being caught, prosecutors say, Schulte declared what he called my information war, and attempted to disclose even more classified information from jail in flagrant defiance of numerous warnings and a court order.Before and after his arrest, prosecutors say, Schulte fed an abhorrent personal fixation through his collection and viewing of an enormous trove of child sexual abuse materials.Approximately 3,400 images and videos were found of what the U.S. attorney's office described as "disturbing and horrific" sex abuse images of children. They were among other images hidden under layers of encryption on a personal computer, the U.S. attorney's office said.After Schulte's prison term, he will be on supervised release for life, the prosecutor's office said.Ken DilanianPhil HelselMay 7, 2017 7:52 AMWikileaks' latest batch of Vault 7 documents focuses on the CIA's anti-forensics toolsCIA logo being cleanedGetty Images / BRENDAN SMIALOWSKI / StringerAfter publishing thousands of politicised emails during the US presidential election, Wikileaks has turned its focus to the US intelligence services.Julian Assange and his team have published more than 8,761 documents that are claimed to be from the US Central Intelligence Agency (CIA).The trove of documents, dubbed Vault 7, is said to be the first of a number of disclosures that reveal the CIA's hacking abilities. "The series is the largest intelligence publication in history," Wikileaks says. "This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive."Here's what you need to know:The fourth release of Wikileak's CIA files, dubbed Grasshopper, dropped on April 7. Within the files are 27 documents, which the leaking organisation says were used by the CIA to build "customised malware payloads for Microsoft Windows operating systems"."Grasshopper is provided with a variety of modules that can be used by a CIA operator as blocks to construct a customised implant that will behave differently, for example maintaining persistence on the computer differently, depending on what particular features or capabilities are selected in the process of building the bundle," Wikileaks says in a statement published alongside the documents.The documents themselves mostly consist of user guides that relate to different computer system modules.For instance, the 107-page Grasshopper-v1_1-AdminGuide explains it defines the modules and payloads needed for a person to build an "operation". Elsewhere, the organisation explains the documents talk about using malware that has been previously used by Russian organised crime units and also provides advice how CIA code can be used to avoid Microsoft security tools.Wikileaks claims the documents provide insights into how the CIA builds "modern espionage tools" and makes use of vulnerabilities in Windows computers.Part three of Wikileak's CIA disclosures, which was first made public on March 31, focuses on the agency's anti-forensics tools called Marble Framework. "Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA," Wikileaks says in its release of the documents.In total Wikieaks has published 676 source code files that it claims are from the CIA. The technology Wikileaks discusses focusses on how the CIA's code is designed to make it easier for those writing malware to disguise who created it.For instance, the leaks organisation says Marble has test examples in multiple languages: it is possible for a person creating malware to set their spoken language as being Chinese, Russian, Korean, Arabic and Farsi. Thus, CIA created malware could potentially be developed to appear as if it was emanating from another country. The CIA has not commented on the disclosures.Wikileaks says: "The Marble source code also includes a deobfuscator to reverse CIA text obfuscation". Unlike previous disclosures in the Vault 7 files, Wikileaks has made the source code for Marble Framework public as it does not specifically contain any vulnerabilities. Previous releases from the files have not included source code as security vulnerabilities have been directly contained within them.Released to the public on March 23, 2017, the second set of documents has been called 'Dark Matter'. Like with part one, it is said to include details of the CIA's global hacking program, and these documents describe hacking methods allegedly used by the agency to access Apple devices and upload data.As WikiLeaks explains: "Dark Matter contains documentation for several CIA projects that infect Apple Mac firmware (meaning the infection persists even if the operating system is re-installed) developed by the CIA's Embedded Development Branch (EDB)."In particular, the documents explain the techniques used by CIA to gain 'persistence' on Apple Mac devices, including Macs and iPhones using, among others, the "Sonic Screwdriver" project. As explained by the CIA, Sonic Screwdriver was a 2012 "mechanism for executing code on peripheral devices while a Mac laptop or desktop is booting". This would allow an attacker to boot its software from a USB stick, for example, "even when a firmware password is enabled".The files reveal the CIA used it to install malware on Thunderbolt-to-Ethernet adaptors, like the Thunderstrike 2 exploit detailed at Black Hat in 2015. Apple fixed the exploit after the Black Hat disclosure meaning the CIA can no longer use that particular exploit to take over Macs.Elsewhere, the DarkSeaSkies project involved "an implant that persists in the EFI firmware of an Apple MacBook Air computer" and consists of "DarkMatter", "SeaPea" and "NightSkies".Apple has responded to the disclosures from Wikileaks by saying it has completed a preliminary investigation on the new information.Based on our initial analysis, the alleged iPhone vulnerability affected iPhone 3G only and was fixed in 2009 when iPhone 3GS was released, the company said in a statement. Additionally, our preliminary assessment shows the alleged Mac vulnerabilities were previously fixed in all Macs launched after 2013.It continued to say it has not negotiated with Wikileaks to be provided with information. Apple said: Thus far, we have not received any information from them that isnt in the public domain.Released to the public on March 7, 2017, the first set of documents was called 'Year Zero' by Wikileaks. Two of the most significant documents showed the CIA's iOS and Android exploits. The iOS issues are detailed here and Android vulnerabilities here.In the iOS documents: the security issues detailed are all given codenames, such as the Elderpiggy, Juggernaut, and Winterspy. Listed in the details are the types of exploit (e.g. API); the types of access the code run (kernel and remote exploits are featured); what version of iOS the flaw works for; descriptions of the issues; and who it was found by (GCHQ, the NSA, and more are featured). Apple has since said the flaws highlighted in the documents had already been fixed in past patches.For Android, there are details on the name, descriptions, proof-of-concept name; what devices are affected; whether it was purchased from a partner; and the type of issue found.However, it isn't just mobile phones that are covered in the documents, web browsers such as Chrome, and even smart TVs have previously undisclosed security vulnerabilities discussed. Google also confirmed that Chrome and Android were not putting people at risk. "Weve reviewed the documents and we're confident security updates and protections in both Chrome and Android already shield users from many of these alleged vulnerabilities," said Heather Adkins, Googles director of information security and privacy."Our analysis is ongoing and we will implement any further necessary protections. We've always made security a top priority and we continue to invest in our defenses."One of the exploits found in smart TVs was called 'Weeping Angel'. The documents show Weeping Angel targeted the Samsung F8000 Smart TV. They say the TV could be turned into "covert listening devices" by putting the TV into "fake-off" mode. When the televisions appeared to be off, it was possible for conversations to be recorded. The CIA documents, which are from 2014, state 'future work' on the vulnerability could include capturing video from the televisions and being able to leave Wi-Fi turned on while 'fake-off' mode was enabled.Critics of the documents' content have said they show how the CIA works with other security agencies around the world to create vulnerabilities that can access the personal data stored on mobile phones and other devices. For instance, NGO Access Now said the CIA should be working with companies. "Many of these vulnerabilities could have been responsibly disclosed and patched," the NGO's senior legislative manager, Nathan White, said in a statement.Also in the documents, the majority of which remain unread and unveiled by journalists, are suggestions that vehicle systems, the Internet of Things and more may be targeted by the CIA in the future.Year Zero also details how the CIA's malware targets Windows, OSx, and Linux routers using USB sticks, software on CDs, and more. It is said CIA rules on how malware should be created include instructions to stop it being tracked back to the US. Wikileaks continued: "CIA hackers developed successful attacks against most well known anti-virus programs".Possibly the biggest question of all. The CIA has neither denied nor confirmed whether the documents are real, saying it does not comment on the "authenticity or content of purported intelligence documents". It is not uncommon for security agencies and law enforcement bodies to take this approach.Former NSA contractor and whistleblower Edward Snowden tweeted to say the documents "look authentic. "Program & office names, such as the JQJ (IOC) crypt series, are real. Only a cleared insider could know them," he wrote.It is well known, from Snowden's own disclosures and also a group called the Shadow Brokers, that US officials can hack into devices and systems. The New York Times says it is "likely" the new Wikileaks' documents are real.Also, Wikileaks has a history of publishing accurate documents obtained from its sources: its Collateral Murder videos showed US military bombing civilians in Iraq.However, Wikileaks, arguably, lost credibility for its connections to Russia; promoting links to databases with sensitive personal information; and defending Milo Yiannopoulos.Paul Calatayud, CTO of FireMon added: The validity of the dumps from my 18 years of experience in cyber, including eight years within the army cyber teams, would lead me to state these claims have basis and are worth taking real consideration over. The tools are very noteworthy yet to be expected if you understand the space."While both Apple and Google said the majority of the issues have been fixed, it is likely there will be more to come in subsequent disclosures.To help the tech firms handle the vulnerabilities, and stop them being exploited once their existence is made public knowledge, Assange has said he will provide the Silicon Valley groups with access to the details.In a press conference on March 10, from London's Ecuadorian embassy, Assange said he had "a lot more information" that would be revealed in the coming weeks and months."After considering what we think is the best way to proceed and hearing these calls from some of the manufacturers," he said. "We have decided to work with them to give them some exclusive access to the additional technical details that we have so that the fixes can be developed and pushed out, so people can be secure".However, the Wikileaks boss did not explain why he had not disclosed the documents to the companies before the release of the 'Year Zero' files. Microsoft told WIRED US it would welcome being contacted but had not been spoken to by Assange.Following publication, the CIA said it will work with the FBI to conduct a criminal investigation into the publication, but both bodies (and the Whitehouse) have declined to comment on the documents' authenticity."The American public should be deeply troubled by any Wikileaks disclosure designed to damage the intelligence community's ability to protect America against terrorists and other adversaries," the CIA told the BBC.Its statement continued: "Such disclosures not only jeopardise US personnel and operations, but also equip our adversaries with tools and information to do us harm."The ex-CIA director Michael Hayden added that the disclosure of the malware and documents, despite redactions of official names, had made the US and other countries "less safe".Included in Vault 7's 'Year Zero' is the suggestion that secure messaging apps using end-to-end encryption had been made vulnerable these include WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman.Security experts have rebutted the claims, saying that the methods listed in the documents involve compromising a mobile device, not the specific apps. Snowden added that the CIA capabilities do not show hacking in the individual apps but the operating systems on mobile devices."There is a big difference between phone operating systems being hacked and message encryption being broken," the UK's Open Rights Group said in a statement. "If a messaging apps encryption has been broken, that would affect every user of the app. The encryption in Signal and WhatsApp has not been broken."This view was supported by other security experts:The UK's secretive spying agency GCHQ and Mi5 are both mentioned within the Vault 7 documents and Wikileaks claims GCHQ developed and gave vulnerabilities to the CIA. The iOS and Android documents list GCHQ as being involved with finding or creating some of the listed vulnerabilities.Within the documents on Weeping Angel, the smart TV hack, UK security agencies are mentioned. "Received sanitised source code from UK with comms and encryption removed," the document says."Programs like Weeping Angel, if true, reveal the broad scope of these arrangements, which continue to operate in secrecy without clear rules or oversight," UK NGO Privacy International, said of the programs.There are a number of unknowns about the documents. The source of the Vault 7 documents is being kept private by Wikileaks but it gives some indication of where they originated.The documents came from a "isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina," it says. Wikileaks continues that the archive had circulated among former US government hackers and contractors with one of them providing the information. All the documents in 'Year Zero' were created between 2013 and 2016."Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete." Within the document redacted names are replaced by 'user numbers'.This article was originally published by WIRED UK WASHINGTON WikiLeaks has published thousands of documents that the anti-secrecy organization said were classified files revealing scores of secrets about CIA hacking tools used to break into targeted computers, cellphones and even smart TVs.The CIA and the Trump administration declined to comment on the authenticity of the files Tuesday, but prior WikiLeaks releases divulged government secrets maintained by the State Department, Pentagon and other agencies that have since been acknowledged as genuine. In another nod to their authenticity, the chairman of the House intelligence committee, Rep. Devin Nunes, R-Calif., said he was very concerned about the release and has sought more information about it.The hacking tools appeared to exploit vulnerabilities in popular operating systems for desktop and laptop computers developed by Microsoft. They also targeted devices that included Apples iPhones and iPads, Googles Android cellphones, Cisco routers and Samsung Smart TVs.Some of the technology firms said they were evaluating the newly released documents.Some questions and answers about the latest WikiLeaks dump and its fallout:Where do these documents come from?WikiLeaks said the material came from an isolated, high-security network inside the CIAs Center for Cyber Intelligence, the spy agencys internal arm that conducts cyber offense and defense. It said the documents were circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. It did not make it clear who was behind the leak, leaving several possibilities: espionage, a rogue employee, a theft involving a federal contractor or a break-in of a staging server where such information may have been temporarily stored.How many files were leaked? What period do they cover?WikiLeaks said 7,818 web pages and 943 attachments were published, but were just the first part of more material to come. WikiLeaks said it has an entire archive of data consisting of several million lines of computer code. The documents appear to date between 2013 and 2016. WikiLeaks described them as the largest-ever publication of confidential documents on the agency.Are these legitimate CIA documents?A spokesman for the CIA said the agency would not comment on the authenticity or content of purported intelligence documents. Trump administration spokesman Sean Spicer declined comment as well. But WikiLeaks has a long track record of assembling and releasing secret files from the U.S. and other governments. Security experts who reviewed the material said the documents appeared to be authentic. Jake Williams, a security expert with Georgia-based Rendition Infosec, who has dealt previously with government hackers, said that frequent references in the files to operation security gave them the stamp of legitimacy. It rings true to me, Williams said.What do these documents contain?The files describe CIA plans and descriptions of malware and other tools that could be used to hack into some of the worlds most popular technology platforms. The documents showed that the developers aimed to be able to inject these tools into targeted computers without the owners awareness.The files do not describe who the prospective targets might be, but the documents show broad exchanges of tools and information between the CIA and National Security Agency and other federal intelligence agencies, as well as intelligence services of close allies Australia, Canada, New Zealand and the United Kingdom.The purported CIA documents range from complicated computer coding to organizational plans to sarcastic comments about the tools effectiveness. Some of the tools were named after alcohol references, including Bartender, Wild Turkey and Margarita. Others referenced recent popular movies, including Fight Club and Talladega Nights. One hacking tool, code-named RickyBobby, after the character who is a race car driver in Talladega Nights, was purportedly used to upload and download information without detection as malicious software.The documents also include discussions about compromising some internet-connected televisions to turn them into listening posts. One document discusses hacking vehicle systems, appearing to indicate the CIAs interest in hacking recent-model cars with sophisticated on-board computer systems.How are technology firms responding to these revelations?Microsoft said it was looking into the reports that its operating systems were potentially vulnerable to many of the malware and other hacking tools described in the purported CIA documents. The maker of the secure messaging app Signal said the purported tools described in the leaked documents appeared to affect users actual phones, but not its software designs or encryption protocols. The manufacturer of the popular Telegram mobile messaging app said in a statement that manufacturers of cellphones and their operating systems, including Apple, Google and Samsung, were responsible for improving the security of their devices. It said the effort will require many hours of work and many security updates and assured its customers that If the CIA is not on your back, you shouldnt start worrying yet. Safeguard the independent, trusted journalism millions rely on at PBS News Hour. 8 March 2017We have no comment on the authenticity of purported intelligence documents released by Wikileaks or on the status of any investigation into the source of the documents. However, there are several critical points we would like to make.CIAs mission is to aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other adversaries. It is CIAs job to be innovative, cutting-edge, and the first line of defense in protecting this country from enemies abroad. America deserves nothing less.It is also important to note that CIA is legally prohibited from conducting electronic surveillance targeting individuals here at home, including our fellow Americans, and CIA does not do so. CIAs activities are subject to rigorous oversight to ensure that they comply fully with U.S. law and the Constitution.The American public should be deeply troubled by any Wikileaks disclosure designed to damage the Intelligence Communitys ability to protect America against terrorists and other adversaries. Such disclosures not only jeopardize U.S. personnel and operations, but also equip our adversaries with tools and information to do us harm.# # # Contents Press Release Analysis Examples Frequently Asked Questions Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election. Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones. Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities. By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified. In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons. Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike. Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective." Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published. Wikileaks has also decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one (Year Zero) already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks. CIA malware targets iPhone, Android, smart TVs CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this organizational chart of the CIA for more details). The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide. The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization. The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server. As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations. The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone. Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, such as iPads. CIA's arsenal includes numerous local and remote "zero days" developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites. A similar unit targets Google's Android which is used to run the majority of the world's smart phones (~85%) including Samsung, HTC and Sony. 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of 2016 the CIA had 24 "weaponized" Android "zero days" which it has developed itself and obtained from GCHQ, NSA and cyber arms contractors. These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied. CIA malware targets Windows, OSx, Linux, routers The CIA also runs a very substantial effort to infect and control Microsoft Windows users with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ("Brutal Kangaroo") and to keep its malware infestations going. Many of these infection efforts are pulled together by the CIA's Automated Implant Branch (AIB), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa". Attacks against Internet infrastructure and webservers are developed by the CIA's Network Devices Branch (NDB). The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are described in the examples section below. CIA 'hoarded' vulnerabilities ("zero days") In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis rather than hoard serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers. Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others. The U.S. government's commitment to the Vulnerabilities Equities Process came after significant lobbying by US technology companies, who risk losing their share of the global market over real and perceived hidden vulnerabilities. The government stated that it would disclose all pervasive vulnerabilities discovered after 2010 on an ongoing basis. "Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals. As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable. The same vulnerabilities exist for the population at large, including the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers. By hiding these security flaws from manufacturers like Apple and Google the CIA ensures that it can hack everyone &mdsh; at the expense of leaving everyone hackable. 'Cyberwar' programs are a serious proliferation risk Cyber 'weapons' are not possible to keep under effective control. While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain. Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost. Securing such 'weapons' is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces sometimes by using the very same 'weapons' against the organizations that contain them. There are substantial price incentives for government hackers and consultants to obtain copies since there is a global "vulnerability market" that will pay hundreds of thousands to millions of dollars for copies of such 'weapons'. Similarly, contractors and companies who obtain such 'weapons' sometimes use them for their own purposes, obtaining advantage over their competitors in selling 'hacking' services. Over the last three years the United States intelligence sector, which consists of government agencies such as the CIA and NSA and their contractors, such as Booz Allan Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers. A number of intelligence community members not yet publicly named have been arrested or subject to federal criminal investigations in separate incidents. Most visibly, on February 8, 2017 a U.S. federal grand jury indicted Harold T. Martin III with 20 counts of mishandling classified information. The Department of Justice alleged that it seized some 50,000 gigabytes of information from Harold T. Martin III that he had obtained from classified programs at NSA and CIA, including the source code for numerous hacking tools. Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike. U.S. Consulate in Frankfurt is a covert CIA hacker base In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa. CIA hackers operating out of the Frankfurt consulate ("Center for Cyber Intelligence Europe" or CCIE) are given diplomatic ("black") passports and State Department cover. The instructions for incoming CIA hackers make Germany's counter-intelligence efforts appear inconsequential: "Breeze through German Customs because you have your cover-for-action story down pat, and all they did was stamp your passport" Your Cover Story (for this trip) Q: Why are you here? A: Supporting technical consultations at the Consulate. Two earlier WikiLeaks publications give further detail on CIA approaches to customs and secondary screening procedures. Once in Frankfurt CIA hackers can travel without further border checks to the 25 European countries that are part of the Shengen open border area including France, Italy and Switzerland. A number of the CIA's electronic attack methods are designed for physical proximity. These attack methods are able to penetrate high security networks that are disconnected from the internet, such as police record database. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The attacker then infects and exfiltrates data to removable media. For example, the CIA attack system Fine Dining, provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a program showing videos (e.g VLC), presenting slides (Prezi), playing a computer game (Breakout2, 2048) or even running a fake virus scanner (Kaspersky, McAfee, Sophos). But while the decoy application is on the screen, the underlaying system is automatically infected and ransacked. How the CIA dramatically increased proliferation risks In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of "Vault 7" the CIA's weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems the agency has little legal recourse. The CIA made these systems unclassified. Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the 'battlefield' of cyber 'war'. To attack its targets, the CIA usually requires that its implants communicate with their control programs over the internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S. Constitution. This means that cyber 'arms' manufactures and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets. Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent. Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable. Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified. A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of military maneuvers against the target's territory including observation, infiltration, occupation and exploitation. Evading forensics and anti-virus A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks. "Tradecraft DO's and DON'Ts" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication (pdf), describing targets & exfiltrated data (pdf) as well as executing payloads (pdf) and persisting (pdf) in the target's machines over time. CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM". CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure. The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools. The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration. Another branch of development focuses on the development and operation of Listening Posts (LP) and Command and Control (C2) systems used to communicate with and control CIA implants; special projects are used to target specific hardware from routers to smart TVs. Some example projects are described below, but see the table of contents for the full list of projects described by WikiLeaks' "Year Zero". UMBRAGE The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity. This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution. The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation. With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from. UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques. Fine Dining Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB (Operational Support Branch) to transform the requests of case officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. The questionnaire allows the OSB to identify how to adapt existing tools for the operation, and communicate this to CIA malware configuration staff. The OSB functions as the interface between CIA operational staff and the relevant technical support staff. Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals. The 'Case Officer' is also asked to specify the environment of the target like the type of computer, operating system used, Internet connectivity and installed anti-virus utilities (PSPs) as well as a list of file types to be exfiltrated like Office documents, audio, video, images or custom file types. The 'menu' also asks for information if recurring access to the target is possible and how long unobserved access to the computer can be maintained. This information is used by the CIA's 'JQJIMPROVISE' software (see below) to configure a set of CIA malware suited to the specific needs of an operation. Improvise (JQJIMPROVISE) 'Improvise' is a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities like Margarita allows the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionairies. HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants. The implants are configured to communicate via HTTPS with the webserver of a cover domain; each operation utilizing these implants has a separate cover domain and the infrastructure can handle any number of cover domains. Each cover domain resolves to an IP address that is located at a commercial VPS (Virtual Private Server) provider. The public-facing server forwards all incoming traffic via a VPN to a 'Blot' server that handles actual connection requests from clients. It is setup for optional SSL client authentication: if a client sends a valid client certificate (only implants can do that), the connection is forwarded to the 'Honeycomb' toolserver that communicates with the implant; if a valid certificate is missing (which is the case if someone tries to open the cover domain website by accident), the traffic is forwarded to a cover server that delivers an unsuspicious looking website. The Honeycomb toolserver receives exfiltrated information from the implant; an operator can also task the implant to execute jobs on the target computer, so the toolserver acts as a C2 (command and control) server for the implant. Similar functionality (though limited to Windows) is provided by the RickBobby project. See the classified user and developer guides for HIVE. Why now? WikiLeaks published as soon as its verification and analysis were ready. In Febuary the Trump administration has issued an Executive Order calling for a "Cyberwar" review to be prepared within 30 days. While the review increases the timeliness and relevance of the publication it did not play a role in setting the publication date. Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete. Over-redaction: Some items may have been redacted that are not employees, contractors, targets or otherwise related to the agency, but are, for example, authors of documentation for otherwise public projects that are used by the agency. Identity vs. person: the redacted names are replaced by user IDs (numbers) to allow readers to assign multiple pages to a single author. Given the redaction process used a single person may be represented by more than one assigned identifier but no identifier refers to more than one real person. Archive attachments (zip, tar.gz, ...) are replaced with a PDF listing all the file names in the archive. As the archive content is assessed it may be made available; until then the archive is redacted. Attachments with other binary content are replaced by a hex dump of the content to prevent accidental invocation of binaries that may have been infected with weaponized CIA malware. As the content is assessed it may be made available; until then the content is redacted. The tens of thousands of routable IP addresses references (including more than 22 thousand within the United States) that correspond to possible targets, CIA covert listening post servers, intermediary and test systems, are redacted for further exclusive investigation. Binary files of non-public origin are only available as dumps to prevent accidental invocation of CIA malware infected binaries. Organizational Chart The organizational chart corresponds to the material published by WikiLeaks so far. Since the organizational structure of the CIA below the level of Directorates is not public, the placement of the EDG and its branches within the org chart of the agency is reconstructed from information contained in the documents released so far. It is intended to be used as a rough outline of the internal organization; please be aware that the reconstructed org chart is incomplete and that internal reorganizations occur frequently. Wiki pages "Year Zero" contains 7818 web pages with 943 attachments from the internal development groupware. The software used for this purpose is called Confluence, a proprietary software from Atlassian. Webpages in this system (like in Wikipedia) have a version history that can provide interesting insights on how a document evolved over time; the 7818 documents include these page histories for 1136 latest versions. The order of named pages within each level is determined by date (oldest first). Page content is not present if it was originally dynamically created by the Confluence software (as indicated on the re-constructed page). What time period is covered? The years 2013 to 2016. The sort order of the pages within each level is determined by date (oldest first). WikiLeaks has obtained the CIA's creation/last modification date for each page but these do not yet appear for technical reasons. Usually the date can be discerned or approximated from the content and the page order. If it is critical to know the exact time/date contact WikiLeaks. What is "Vault 7" "Vault 7" is a substantial collection of material about CIA activities obtained by WikiLeaks. When was each part of "Vault 7" obtained? Part one was obtained recently and covers through 2016. Details on the other parts will be available at the time of publication. Is each part of "Vault 7" from a different source? Details on the other parts will be available at the time of publication. What is the total size of "Vault 7"? The series is the largest intelligence publication in history. How did WikiLeaks obtain each part of "Vault 7"? Sources trust WikiLeaks to not reveal information that might help identify them. Isn't WikiLeaks worried that the CIA will act against its staff to stop the series? No. That would be certainly counter-productive. Has WikiLeaks already 'mined' all the best stories? No. WikiLeaks has intentionally not written up hundreds of impactful stories to encourage others to find them and so create expertise in the area for subsequent parts in the series. They're there. Look. Those who demonstrate journalistic excellence may be considered for early access to future parts. Won't other journalists find all the best stories before me? Unlikely. There are very considerably more stories than there are journalists or academics who are in a position to write them. In 2017,

amidst the usual buzz of pop culture and global events, a seismic shift occurred in the world of intelligence. While Beyoncs pregnancy announcement and the Super Bowl dominated headlines, Wikileaks quietly set off a bombshell that would shake the foundations of global cybersecurity and espionage. Through a series of cryptic tweets, Wikileaks introduced the world to "Vault 7," a collection of leaked CIA documents that revealed the extent of the agency's cyber-espionage operations. The revelations not only exposed the CIAs covert activities but also sparked debates about privacy, national security, and the ethics of state-sponsored hacking.Whisteblower Edward Snowden has tweeted that the leak appears to be authenticThe Prelude: Cryptic Tweets and Conspiracy TheoriesOn February 4, 2017, Wikileaks began a cryptic Twitter campaign that left the online world abuzz with speculation. The initial tweet asked, "What is Vault 7?" and was accompanied by an image of the Global Seed Vault in Norway, a facility often linked to conspiracy theories. Each day, Wikileaks released a new tweet paired with an enigmatic photograph: a Nazi gold vault, an engine test at Langley Air Force Base, fake newspaper covers, and finally, a woman mailing a letter under surveillance by the East German secret police.The internet erupted with theories. Some believed it was a continuation of the Hillary Clinton email saga, while others thought it might be connected to World Trade Center Building 7 or even the cryptographic puzzle organization Cicada 3301. However, the true nature of Vault 7 remained a mystery until March 7, 2017, when Wikileaks unveiled the full scope of its leak.The official Vault 7 logo used by Wikileaks during the releaseVault 7: Year ZeroOn March 7, 2017, Wikileaks released a torrent link to an encrypted set of files labeled "Vault 7: Year Zero." The following day, they tweeted the passphrase needed to decrypt the filesa famous John F. Kennedy quote: "SplinterItIntoAThousandPiecesAndScatterItIntoTheWinds." With this release, Wikileaks disclosed 8,761 CIA documents detailing the agencys cyber-espionage tools and techniques developed between 2008 and 2016. This was the largest leak of classified intelligence documents in history.Wikileaks reveals the decryption passphrase for Vault 7: Year ZeroThe Tools of EspionageThe Vault 7 documents revealed a vast array of tools and exploits used by the CIA to infiltrate and control electronic devices around the world. Some of the most notable tools included:Weeping Angel: A software developed in partnership with the UK's MI5 that turned Samsung smart TVs into covert listening devices, even when they appeared to be off.Sonic Screwdriver: A tool that allowed the CIA to execute malicious code on Mac computers during their boot process, bypassing security measures and maintaining control over the system.Hive: A command and control framework that enabled the CIA to manage malware implants on compromised systems and extract sensitive information covertly.Scribbles: A tool designed to embed tracking beacons in documents likely to be stolen, allowing the CIA to monitor who accessed the files.These tools, along with many others detailed in the leak, demonstrated the CIA's ability to carry out sophisticated cyber-attacks, often using techniques that left little trace of their origin. The documents also revealed that the CIA had a practice of stealing malware from other nations, such as Russia, and repurposing it for their own operations to mislead forensic investigators.Diagram of the Hive Command and Control Framework from the Vault 7 documentsThe Fallout and ConsequencesThe immediate aftermath of the Vault 7 release was chaotic. The CIA, forced to acknowledge the leak, faced significant embarrassment and criticism for its security practices. Wikileaks founder Julian Assange held a press conference, where he condemned the CIA for hoarding vulnerabilities rather than disclosing them to software manufacturers, thus putting the public at risk.A criminal investigation was quickly launched in the United States, focusing on identifying the source of the leak. Joshua Schulte, a former CIA software engineer, was arrested and later charged in connection with the leak. Schultes trial was fraught with controversy, including allegations of his involvement in illegal activities unrelated to the leak, which further complicated the case.In this courtroom sketch, Joshua Schulte, center, is seated at the defense table flanked by his attorneys during jury deliberations, March 4, 2020, in New YorkThe Legacy of Vault 7Vault 7 remains one of the most significant intelligence leaks in history, shedding light on the dark world of state-sponsored hacking and cyber-espionage. The release not only exposed the CIAs methods but also raised important questions about the balance between national security and privacy in the digital age.For those interested in delving deeper into the Vault 7 documents, they remain available for public download. You can access them via the original torrent link provided by Wikileaks: Download Vault 7: Year Zero, using the passphrase: SplinterItIntoAThousandPiecesAndScatterItIntoTheWinds.For a more detailed exploration of the events surrounding the Vault 7 leak, you can watch the video that delves into the story of Joshua Schulte and the repercussions of his actions: When a CIA Hacker Goes Rogue.Disclaimer: The documents discussed in this article are publicly available, and the analysis provided here is for informational purposes only.

Used versatile tractors for sale in saskatchewan. Versatile tractors for sale in sask.

- liwaxota
- gezihazo
- how to set up miller bobcat 225
- hokowopu
- pevewasu
- xifereceru
- https://eksenmermer.com/ckfinder/userfiles/files/12016540676.pdf
- what is a motor vehicle repairers licence
- kiyoda
- pirate chain crypto price
- https://sbriz.ru/userfiles/file/24d3a2be-a252-47a8-a9a3-27096901c527.pdf
- where does eurostar leave uk